Revista Brasileira de História da Matemática - Vol. 14 nº 28 - pág. 115-126
Publicação Oficial da Sociedade Brasileira de História da Matemática
ISSN 1519-955X

"INVESTIGAÇÕES SOBRE OS MEIOS DE RECONHECER SE UM PROBLEMA DE GEOMETRIA PODE SER RESOLVIDO COM A RÉGUA E O COMPASSO" DE PIERRE LAURENT WANTZEL - TRADUÇÃO

Fernando Raul Neto
Universidade Federal de Pernambuco – UFPE – *Brasil*

João Paulo Barbosa
Universidade de Pernambuco – UPE – *Brasil*

(aceito para publicação em abril de 2014)

Tradução[1]

I.

Suponhamos que um problema de Geometria possa ser resolvido por meio de intersecções de linhas retas e de circunferências de círculo: se juntarmos os pontos assim obtidos com os centros dos círculos e com os pontos que determinam as retas, formar-se-á um encadeamento de triângulos retilíneos cujos elementos podem ser calculados pelas fórmulas da Trigonometria; além disso, essas fórmulas são equações algébricas que contém os lados e as linhas trigonométricas dos ângulos elevados apenas ao primeiro e ao segundo graus; assim, a incógnita principal do problema será obtida pela resolução de uma série de equações do segundo grau cujos coeficientes serão funções racionais dos dados da questão e das raízes das equações precedentes. Dessa forma, para reconhecer se a construção de um problema de geometria pode ser realizada com a régua e o compasso, é preciso verificar se é possível reduzir as raízes da equação do problema àquelas de um sistema de equações do segundo grau obtido da forma como indicamos. Trataremos aqui exclusivamente do caso em que a equação do problema é algébrica.

II.

Consideremos o sistema (A) de equações:

[1] O artigo *Recherches sur les moyens de reconnaître si um Problème de Géométrie peut se résoudre avec la règle et le compas* do matemático francês Pierre Laurent Wantzel (1814, 1848) foi publicado em Paris, em 1837, nas páginas 366 - 372 do volume 2 do *Journal de Mathématiques pures et appliquées.* O artigo é uma referencia obrigatória para aqueles que se interessam pela história das construções geométricas com régua e compasso, particularmente sobre a impossibilidade da duplicação do cubo e da trissecção do ângulo.

$$\text{(A)} \qquad \begin{cases} x_1^2 + Ax_1 + B = 0,\ x_2^2 + A_1x_2 + B_1 = 0 \ \ldots, \\ x_{n-1}^2 + A_{n-2}x_{n-1} + B_{n-2} = 0,\ x_n^2 + A_{n-1}x_n + B_{n-1} = 0. \end{cases}$$

nas quais A e B representam funções racionais das quantidades dadas p, q, r ... ; A_1 e B_1, funções racionais de x_1, p, q, ... ; e, em geral, A_m e B_m funções racionais de x_m, x_{m-1}, ... x_1, p, q ... .

Toda função racional de x_m, como A_m ou B_m, toma a forma $\frac{C_{m-1}x_m + D_{m-1}}{E_{m-1}x_m + F_{m-1}}$ quando as potencias de x_m superiores à primeira são eliminadas por meio da equação $x_m^2 + A_{m-1}x_m + B_{m-1} = 0$, C_{m-1}, D_{m-1}, E_{m-1}, F_{m-1} designando funções racionais de x_{m-1}, ... x_1, p, q ... ; Em seguida, ela pode ser reduzida à forma $A'_{m-1}x_m + B'_{m-1}$ ao multiplicarmos os dois termos de $\frac{C_{m-1}x_m + D_{m-1}}{E_{m-1}x_m + F_{m-1}}$ por $-E_{m-1}(A_{m-1} + D_m) + F_{m-1}$.

Multipliquemos um pelo outro os dois valores que toma o primeiro membro da última das equações *(A)* quando substituimos x_{n-1} em A_{n-1} e B_{n-1}, sucessivamente, pelas duas raízes da equação precedente: obteremos um polinômio do quarto grau em x_n cujos coeficientes se exprimirão como função racional de x_{n-2} ... x_1, p, q, ... Substituindo da mesma maneira, sucessivamente, nesse polinômio, x_{n-2} pelas duas raízes da equação correspondente, obteremos dois resultados cujo produto será um polinômio em x_n de grau 2^3 e cujos coeficientes serão funções racionais de x_{n-3} ... x_1, p, q ... . Continuando da mesma maneira, chegaremos a um polinômio em x_n de grau 2^n, cujos coeficientes serão funções racionais de p, q, r ... . Esse polinômio igualado a zero dará a equação final $f(x_n) = 0$ ou $f(x) = 0$, que engloba todas as soluções da questão. Podemos sempre supor que, antes de efetuar o cálculo, as equações (A) foram reduzidas ao menor número possível. Dessa forma, uma equação qualquer entre elas, como $x_{m+1}^2 + A_m x_{m+1} + B_m = 0$, não pode ser satisfeita por uma função racional das quantidades dadas e das raízes das equações precedentes. Pois, se assim fosse, o resultado da substituição seria uma função racional de x_m, ... x_1, p, q ... que podemos colocar sob a forma $A'_{m-1}x_m + B'_{m-1}$ e obteríamos $A'_{m-1}x_m + B'_{m-1} = 0$; Dessa relação encontraríamos um valor racional de x_m que substituído na equação do segundo grau em x_m conduziria a um resultado da forma $A'_{m-2}x_{m-1} + B'_{m-2} = 0$. Continuando assim, se chegaria à $A'x_1 + B' = 0$, isto é, que a equação $x_1^2 + Ax_1 + B = 0$ teria por raízes funções racionais de p, q ... . O sistema de equações (A) poderia então ser substituído por dois sistemas de $n-1$ equações do segundo grau, independentes um do outro, o que é contra a hipótese. Se uma das relações intermediárias $A'_{m-2}x_{m-1} + B'_{m-2} = 0$, por exemplo, fosse satisfeita identicamente, as duas raízes da equação $x_{m-1}^2 + A_{m-1}x_m + B_{m-1} = 0$ seriam funções racionais de x_{m-1} ... x_1, para todos os valores que podem assumir essas quantidades, de maneira que se poderia suprimir a equação x_m e substituir a raiz sucessivamente pelos seus dois valores nas equações seguintes, o que levaria ainda o sistema das equações (A) a dois sistemas de $n-1$ equações.

III.

Isso posto, *a equação de grau* 2^n, $f(x) = 0$, *que fornece todas as soluções de um problema suscetível de ser resolvido por meio de n equações do segundo grau é, necessariamente, irredutível*, isto é, não pode ter raízes comuns com uma equação de grau

menor cujos coeficientes sejam funções racionais dos dados p, q ... .

Com efeito, suponhamos que uma equação $F(x) = 0$, com coeficientes racionais, seja satisfeita por uma raiz da equação $x_n^2 + A_{n-1}x_n + B_{n-1} = 0$, atribuindo certos valores convenientes às quantidades $x_{n-1}, x_{n-2} \ldots x_1$. A função racional $F(x_n)$ de uma raiz dessa última equação pode ser escrita na forma $A'_{n-1}x_n + B'_{n-1,}$ designando sempre por A'_{n-1} *e* B'_{n-1} as funções racionais de x_{n-1} ... x_1, p, q ... . Da mesma forma, tanto A'_{n-1} como B'_{n-1} podem ser escritas na forma $A'_{n-2}x_{n-1} + B'_{n-2}$, e assim sucessivamente. Chega-se assim a $A'_1x_2 + B'_{1,}$ onde A'_1 e B'_1 podem ser colocados sob a forma $A'x_1 + B'$ na qual A'e B' representam funções racionais dos dados *p, q* ... . Como $F(x_n) = 0$ para um dos valores de x_n, teríamos $A'_{n-1}x_n + B'_{n-1} = 0$, e seria preciso que A'_{n-1} e B'_{n-1} fossem nulos isoladamente, sem o que a equação $x_n^2 + A_{n-1}x_n + B_{n-1} = 0$ seria satisfeita pelo valor $-\frac{B'_{n-1}}{A'_{n-1}}$ que é uma função racional de x_{n-1} ... x_1, p, q ..., o que é impossível. Da mesma maneira, sendo A'_{n-1} e B'_{n-1} nulos, A'_{n-2} e B'_{n-2} também seriam nulos e assim sucessivamente até A' e B' que seriam nulos identicamente, pois eles não contém mais que as quantidades dadas. Mas então A'_1 e B'_1, que tomam igualmente a forma $A'x_1 + B'$ quando se substitui por x_1 cada uma das raízes da equação $x_1^2 + Ax_1 + B = 0$, se anulariam para esses dois valores de x_1. Da mesma forma, os coeficientes A'_2 e B'_2 podem ser colocados sob a forma $A'_1x_2 + B'_1$, tomando por x_2 uma ou outra das raízes da equação $x_2^2 + A_1x_2 + B_1 = 0$, correspondentes a cada um dos valores x_1, e por consequência eles se anularão para os quatro valores de x_2 e para os dois valores de x_1 que resultam da combinação das duas primeiras equações (A). Demonstra-se da mesma forma que A'_3 e B'_3 serão nulos ao substituir por x_3 os 2^3 valores tirados das três primeiras equações (A) conjuntamente com os valores correspondentes de x_2 e x_1. Continuando dessa maneira, se concluirá que $F(x_n)$ se anulará para os 2^n valores de x_n aos quais conduz o sistema de todas as equações (A) ou para as 2^n raízes de $f(x) = 0$. Assim uma equação $F(x) = 0$ com coeficientes racionais não pode admitir uma raiz de $f(x) = 0$ sem admitir todas. Portanto a equação $f(x) = 0$ é irredutível.

IV.

Resulta imediatamente do teorema precedente que todo problema que conduz a uma equação irredutível cujo grau não é uma potencia de *2*, não pode ser resolvido com a linha reta e o círculo. Dessa forma a *duplicação do cubo*, que depende da equação $x^3 - 2a^3 = 0$, sempre irredutível, não pode ser obtida pela Geometria elementar. O problema *das duas médias proporcionais*, que conduz à equação $x^3 - a^2b = 0$, cai no mesmo caso, todas as vezes que a razão de *b* para *a* não é um cubo. A *trissecção do ângulo* depende da equação $x^3 - \frac{3}{4}x + \frac{1}{4}a = 0$ e ela é irredutível, se não possuir raiz que seja uma função racional de *a*, e é esse o caso desde que *a* seja algébrico. Assim o problema não pode ser resolvido em geral com a régua e o compasso. Nos parece que ainda não havia sido demonstrado rigorosamente que esses problemas, tão célebres entre os antigos, não eram suscetíveis de uma solução pelas construções geométricas aos quais eles particularmente devem sua origem.

A divisão da circunferência em partes iguais pode sempre ser reduzida à resolução da equação $x^m - 1 = 0$, na qual *m* é um número primo ou uma potencia de um número

primo. Quando m é primo, a equação $\frac{x^m - 1}{x - 1} = 0$ de grau $m - 1$ é irredutível, como Gauss havia mostrado em suas *Disquisitiones arithmeticae*, seção VII. Assim a divisão não pode ser efetuada pelas construções geométricas, salvo se $m - 1 = 2^\alpha$. Quando m é da forma a^α, pode-se provar, modificando ligeiramente a demonstração de Gauss, que a equação de grau $(a-1)a^{\alpha-1}$, obtida igualando a zero o quociente de $x^{a^\alpha} - 1$ por $x^{a^{\alpha-1}} - 1$, é irredutível. Seria necessário, portanto, que $(a-1)a^{\alpha-1}$ fosse da forma 2^n ao mesmo tempo que $a - 1$, o que é impossível, a menos que $a = 2$. Assim *a divisão da circunferência em N partes não pode ser efetuada com a régua e o compasso, salvo se os fatores primos de N diferentes 2 sejam da forma* $2^n + 1$ *e se eles entram unicamente como primeira potencia desse número*. Esse princípio é trazido por Gauss ao final de sua obra, mas ele não forneceu a demonstração.

Se $x = k + A'\sqrt[m']{a'} + A''\sqrt[m'']{a''} + etc.$, sendo m', m'', ... potencias de *2*, e *k*, A', A'', ... a', a'', ... números comensuráveis, o valor de *x* se construirá com a linha reta e o círculo, de maneira que *x* não pode ser raiz de uma equação irredutível de grau *m* que não seja uma potencia de *2*. Por exemplo, não se pode ter $x = A\sqrt[m]{a}$, se $\left(\sqrt[m]{a}\right)^p$ é irracional para $p < m$. Demonstra-se facilmente que *x* não pode tomar aquele valor, mesmo que *m* fosse uma potencia de 2. Encontramos assim vários casos particulares de teoremas sobre números incomensuráveis que já havíamos estabelecido em outro local.[*]

V.

Suponhamos que um problema tenha conduzido à uma equação F(x) = 0 de grau 2^n e que esteja assegurado que essa equação é irredutível. Trata-se de saber se a solução pode ser obtida por meio de uma série de equações do segundo grau.

Retomemos as equações (A):

(A) $$\begin{cases} x_1^2 + Ax_1 + B = 0,\ x_2^2 + A_1x_2 + B_1 = 0\ \ldots, \\ x_{n-1}^2 + A_{n-2}x_{n-1} + B_{n-2} = 0,\ x_n^2 + A_{n-1}x_n + B_{n-1} = 0. \end{cases}$$

É preciso construir a equação $f(x) = 0$, com coeficientes racionais, que forneça todos os valores de x_n e identificá-la com a equação dada $F(x) = 0$. Para efetuar esse cálculo, observa-se que A_{n-1} e B_{n-1} se reduzem à forma $a_{n-1}x_{n-1} + a'_{n-1}$ e $b_{n-1}x_{n-1} + b'_{n-1}$ e que a eliminação de x_{n-1} nessas duas últimas equações (A) se faz imediatamente, o que dá uma equação de quarto grau em x_n. Substitui-se em seguida a_{n-1} por $a''_{n-1}x_{n-2} + a'''_{n-1}$, a'_{n-1} por $a^{iv}_{n-1}x_{n-2} + a^v_{n-1}$, b_{n-1} por $b''_{n-1}x_{n-2} + b'''_{n-1}$, b'_{n-1} por $b^{iv}_{n-1}x_{n-2} + b^v_{n-1}$ e A_{n-2}, B_{n-2} por $a_{n-2}x_{n-2} + a'_{n-2}$, $b_{n-2}x_{n-2} + b'_{n-2}$ e, em seguida, elimina-se x_{n-2} entre as equações do 4° grau já obtidas e a equação $x_{n-2}^2 + A_{n-3}x_{n-2} + B_{n-3} = 0$; e assim sucessivamente. Os últimos termos das séries a_{n-1}, a'_{n-1}, a''_{n-1} ..., b_{n-1}, b'_{n-1}..., etc., devem ser funções racionais dos coeficientes de $F(x) = 0$. Se puderms lhes atribuir valores racionais que satisfazem as equações de condição obtidas na identificação, se reproduzirá o sistema de equações (A) que equivale à equação $F(x) = 0$. Se as condições não puderem ser verificadas atribuindo valores racionais às indeterminadas introduzidas, o problema não pode ser reduzido ao segundo grau.

[*] Jounal de L'École Polytechnique, Cahier XXVI.

Pode-se simplificar esse procedimento supondo que as raízes da cada uma das equações (A) dão o último termo da seguinte. Dessa forma, pode-se tomar B_{n-1} como incógnita da penúltima equação, pois $B_{n-1} = b_{n-1}x_{n-1} + b'_{n-1}$, de onde segue que $x_{n-1} = \frac{B_{n-1} - b'_{n-1}}{b_{n-1}}$. Dessa maneira as eliminações se fazem mais rapidamente, e se introduz quatro quantidades indeterminadas na equação do quarto grau que resulta da primeira eliminação, oito na equação de oitavo grau, etc., de modo que as condições obtidas na identificação são em mesmo número que as quantidades a determinar. Mas descarta-se também, de início, o caso no qual uma das quantidades como b_{n-1} fosse nula. Seria necessário estudar esse caso separadamente.

Seja, por exemplo, a equação $x^4 + px^2 + qx + r = 0$. Tomemos em seguida as equações do segundo grau sob a forma $x_1^2 + Ax_1 + B = 0$ e $x^2 + (ax_1 + a')x + x_1 = 0$; eliminando x_1 e igualando, obtemos,

$2a' - Aa = 0, a'^2 - Aaa' - A + a^2B = p, 2aB - a'A = q, B = r,$

de onde segue

$B = r, a = \frac{2q}{4r - A^2}, a' = \frac{Aq}{4r - A^2}, A^3 + pA^2 - 4rA + q^2 - 4rp = 0.$

Como *B*, a e a' estão expressos racionalmente por meio de *A*, *p*, *q*, *r*, é necessário e suficiente que a equação do terceiro grau em *A* tenha por raiz uma função racional dos dados. A condição é sempre satisfeita quando $q = 0$, quaisquer que sejam p e *r*, pois $A = -p$ satisfaria a última equação

Tomando x_1 como último termo da segunda equação do segundo grau, exclui-se o caso onde esse termo seria independente da raiz da primeira equação. Mas tratando-o diretamente, não se encontra solução alguma para a questão que não esteja incluída nas equações acima.

Dessa forma, por meio de um cálculo mais ou menos longo, poder-se-ia sempre se assegurar se um problema dado é suscetível de ser resolvido por meio de uma série de equações do segundo grau, desde que se saiba reconhecer se uma equação pode ser satisfeita por uma função racional dos dados, e se ela é irredutível. Uma equação do grau *n* será irredutível quando entre os divisores dos termos do primeiro membro de graus *1, 2, ...* $\frac{n}{2}$, não se encontre nenhum cujos coeficientes sejam funções racionais das quantidades dadas.

A questão pode assim sempre ser reduzida a determinar se uma equação algébrica $F(x) = 0$ com uma única incógnita pode ter como raiz uma função desse tipo. Para isso, há vários casos a considerar. 1º Se os coeficientes só dependem dos números dados, inteiros ou fracionários, é suficiente aplicar o método das raízes comensuráveis. 2º Pode ocorrer que os dados representados pelas letras *p, q, r* sejam suscetíveis de tomar uma infinidade de valores, sem que a condição deixe de ser cumprida, como quando ela designa várias linhas tomadas arbitrariamente. Então, após reduzir a equação *F(x) = 0* a uma forma tal que seus coeficientes sejam frações inteiras de *p, q, r ...*, e que aquele do primeiro termo seja a unidade, se substituirá *x* por $a_m p^m - a_{m-1}p^{m-1} + \ldots + a_0$, e se igualará a zero os coeficientes das diferentes potencias no resultado. As equações obtidas em a_m, a_{m-1} ... serão tratadas como uma equação em *x*, isto é, que se substituirá essas quantidades pelas funções inteiras de *q*, e assim sucessivamente até que tendo exaurido todas as letras se

chegue as equações numéricas que levam ao primeiro caso. 3º Quando os dados são números irracionais, eles devem ser raízes de equações algébricas que pode-se supor irredutíveis. Nesse caso, se substituirmos *x* por $a_m p^m + \ ... + a_0$ em $F(x) = 0$, o primeiro membro da equação em p assim obtida deverá ser divisível por aquele da equação irredutível que possui p por raiz. Supondo que essa divisão se faça exatamente, se chegará as equações em a_m, a_{m-1} ..., que se tratará como a equação $F(x) = 0$ até que se chegue às equações numéricas. Deve-se salientar que *m* pode sempre ser tomado inferior ao grau da equação que fornece p.

Esses procedimentos são em geral laboriosos de aplicar, mas é possível simplificá-los e obter resultados mais precisos em alguns casos mais gerais que, particularmente, estudaremos.

Transcrição

Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas

Pierre Laurent Wantzel

I.

Supposons qu'un problème de Géométrie puisse être résolu par des intersections de lignes droites et de circonférences de cercle: si l'on joint les points ainsi obtenus avec les centres des cercles et avec les points qui déterminent les droites on formera un enchaînement de triangles rectilignes dont les éléments pourront être calculés par les formules de la Trigonométrie; d'ailleurs ces formules sont des équations algébriques qui ne renferment les côtés et les lignes trigonométriques des angles qu'au premier et au second degré; ainsi l'inconnue principale du problème s'obtiendra par la résolution d'une série d'équations du second degré dont les coefficients seront fonctions rationnelles des données de la question et des racines des équations précédentes. D'après cela, pour reconnaître si la construction d'un problème de Géométrie peut s'effectuer avec la règle et le compas, il faut chercher s'il est possible de faire dépendre les racines de l'équation à laquelle il conduit de celles d'un système d'équations du second degré composées comme on vient de l'indiquer. Nous traiterons seulement ici le cas où l'équation du problème est algébrique.

II.

Considérons la suite d'équations:

$$(A)\begin{cases} x_1^2 + \mathrm{A}x_1 + \mathrm{B} = 0, x_2^2 + A_1 x_2 + B_1 = 0 \ldots x_{n-1}^2 + A_{n-2}x_{n-1} + B_{n-2} = 0 \\ x_n^2 + A_{n-1}x_n + B_{n-1} = 0, \end{cases}$$

dans lesquelles *A* et *B* représentent des fonctions rationnelles des quantités données *p*, *q*, *r* ... ; A_1 et B_1, des fonctions rationnelles de x_1, *p*, *q*, ... ; et, en général, A_m et B_m des fonctions rationnelles de $x_m, x_{m-1}, \ldots x_1$, p, q ... .

Toute fonction rationnelle de x_m telle que A_m ou B_m, prend la forme $\frac{\mathrm{C_{m-1}x_m + D_{m-1}}}{\mathrm{E_{m-1}x_m + F_{m-1}}}$ si l'on élimine les puissances de x_m supérieures à la première au moyen de l'équation $x_m^2 + A_{m-1}x_m + B_{m-1} = 0$,[2] en désignant par C_{m-1}, D_{m-1}, E_{m-1}, F_{m-1} des fonctions rationnelles de x_{m-1}, ... x_1, *p*, *q* ... ; elle se ramènera ensuite à la forme $A'_{m-1}x_m + B'_{m-1}$en multipliant les deux termes de $\frac{\mathrm{C_{m-1}x_m + D_{m-1}}}{\mathrm{E_{m-1}x_m + F_{m-1}}}$ par $-E_{m-1}(A_{m-1} + D_m) + F_{m-1}$.

Multiplions l'une par l'autre les deux valeurs que prend le premier membre de la dernière des équations *(A)* lorsqu'on met successivement à la place de x_{n-1} dans A_{n-1} et B_{n-1} les deux racines de l'équation précédente: nous aurons un polynome du quatrième degré en x_n dont les coefficients s'exprimeront en fonction rationnelle de x_{n-2} ... x_1, *p*, *q*, ... ; remplaçons de même successivement dans ce polynome x_{n-2} par les deux racines de l'équation correspondante, nous obtiendrons deux résultats dont le produit sera un polynome em x_n de degré 2^3, à coefficient rationnel par rapport à x_{n-3} ... x_1, *p*, *q* ... ; et, en continuant de la même manière, nous arriverons à un polynome en x_n de degré 2^n dont les

[2] No original a_{m-1}, ao invés de A_{m-1}.

coefficients seront des fonctions rationnelles de p, q, r ... . Ce polynome égalé à zéro donnera l'équation finale $f(x_n) = 0$ ou $f(x) = 0$, qui renferme toutes les solutions de la question. On peut toujours supposer qu'avant de faire le calcul on a réduit les équations *(A)* au plus petit nombre possible. Alors une quelconque d'entre elles $x_{m+1}^2 + A_m x_{m+1} + B_m = 0$, ne peut pas être satisfaite par une fonction rationnelle des quantités données et des racines des équations précédentes. Car, s'il en était ainsi, le résultat de la substitution serait une fonction rationnelle de x_m, ... x_1, p, q ... qu'on peut mettre sous la forme $A'_{m-1}x_m + B'_{m-1}$ et l'on aurait $A'_{m-1}x_m + B'_{m-1} = 0$; on tirerait de cette relation une valeur ratiounelle de x_m qui substituée dans l'équation du second degré en x_m conduirait à un résultat de la forme $A'_{m-2}x_{m-1} + B'_{m-2} = 0$. En continuant ainsi, on arriverait a $A'x_1 + B' = 0$, c'est-à-dire que l'équation $x_1^2 + Ax_1 + B = 0$ aurait pour racines des fonctions rationnelles de p, q ... ; le système des équations *(A)* pourrait donc être remplacé par deux systèmes de $n - 1$ équations du second degré, indépendants l'un de l'autre, ce qui est contre la supposition. Si l'une des relations intermédiaires $A'_{m-2}x_{m-1} + B'_{m-2} = 0$, par exemple, était satisfaite identiquement, les deux racines de l'équation $x_{m-1}^2 + A_{m-1}x_m + B_{m-1} = 0$ seraient des fonctions rationnelles de x_{m-1} ... x_1, pour toutes les valeurs que peuvent prendre ces quantités, en sorte qu'on pourrait supprimer l'équation en x_m et remplacer la racine successivement par ses deux valeurs dans les équations suivantes, ce qui ramènerait encore le système des équations *(A)* à deux systèmes de $n - 1$ équations.

III.

Cela posé, *l'équation du degré* 2^n, $f(x) = 0$, *qui donne toutes les solutions d'un problème susceptible d'être résolu au moyen de n équations du second degré, est nécessairement irréductible*, c'est-à-dire qu'elle ne peut avoir de racines communes avec une équation de degré moindre dont les coefficients soient des fonctions rationnelles des données p, q ... .

En effet, supposons qu'une équation $F(x) = 0$, à coefficients rationnels soit satisfaite par une racine de l'équation $x_n^2 + A_{n-1}x_n + B_{n-1} = 0$, en attribuant certaines valeurs convenables aux quantités $x_{n-1}, x_{n-2} \ldots x_1$. La fonction rationnelle $F(x_n)$ d'une racine de cette dernière équation peut se ramener à la forme $A'_{n-1}x_n + B'_{n-1}$, en désignant toujours par A'_{n-1} *et* B'_{n-1} des fonctions rationnelles de x_{n-1} ... x_1, p, q ... ; de même A'_{n-1} et B'_{n-1} peuvent prendre l'un et l'autre la forme $A'_{n-2}x_{n-1} + B'_{n-2}$,[3] et ainsi de suite; on arrivera ainsi à $A'_1x_2 + B'_1$ où A'_1 et B'_1 peuvent être mis sous la forme $A'x_1 + B'$dans laquelle A'et B' représentent des fonctions rationnelles des données p, q ... . Puisque $F(x_n) = 0$ pour une des valeurs de x_n, on aura $A'_{n-1}x_n + B'_{n-1} = 0$,[4] et il faudra que A'_{n-1} et B'_{n-1} soient nuls séparément, sans quoi l'équation $x_n^2 + A_{n-1}x_n + B_{n-1} = 0$ serait satisfaite pour la valeur $-\frac{B'_{n-1}}{A'_{n-1}}$ qui est une fonction rationnelle de.. x_{n-1} ... x_1, p, q ..., ce qui est impossible; de même, A'_{n-1}[5] et B'_{n-1} étant nuls, A'_{n-2} et B'_{n-2} le seront aussi et ainsi de suite jusqu'à A' et B' qui seront nuls identiquement, puisqu'ils ne renferment que des quantités données. Mais alors A'_1 e B'_1, qui prennent également la forme $A'x_1 + B'$ quand on

[3] No original B'_{n-1}.
[4] No original A'_{-1}.
[5] No original A'_{-1}.

met pour x_1 chacune des racines de l'équation $x_1^2 + Ax_1 + B = 0$, s'annuleront pour ces deux valeurs de x_1; pareillement, les coefficients A_2' et B_2' peuvent être mis sous la forme $A_1'x_2 + B_1'$, en prenant pour x_2 l'une ou l'autre des racines de l'équation $x_2^2 + A_1x_2 + B_1 = 0$, correspondantes à chacune des valeurs de x_1, et par conséquent ils s'annulleront pour les quatre valeurs de x_2 et pour les deux valeurs de x_1 qui résultent de la combinaison des deux premières équations *(A)*. On démontrera de même que A_3' et B_3' seront nuls en mettant pour x_3 les 2^3 valeurs tirées des trois premières équations *(A)* conjointement avec les valeurs correspondantes de x_2 et x_1; et continuant de cette manière on conclura que $F(x_n)$ s'annulera pour les 2^n valeurs de x_n auxquelles conduit le système de toutes les équations *(A)* ou pour les 2^n racines de $f(x) = 0$. Ainsi une équation $F(x) = 0$ à coefficients rationnels ne peut admettre une racine de $f(x) = 0$ sans les admettre toutes; donc l'équation $f(x) = 0$ est irréductible.

IV.

Il résulte immédiatement du théorème précédent que tout problème qui conduit à une équation irréductible dont le degré n'est pas une puissance de *2*, ne peut être résolu avec la ligne droite et le cercle. Ainsi *la duplication du cube*, qui dépend de l'équation $x^3 - 2a^3 = 0$ toujours irréductible, ne peut être obtenue par la Géométrie élémentaire. Le problème *des deux moyennes proportionnelles*, qui conduit à l'équation $x^3 - a^2b = 0$ est dans le même cas toutes les fois que le rapport de *b* à *a* n'est pas un cube. La *trisection de l'angle* dépend de l'équation $x^3 - \frac{3}{4}x + \frac{1}{4}a = 0$; cette équation est irréductible si elle n'a pas de racine qui soit une fonction rationnelle de *a* et c'est ce qui arrive tant que *a* reste algébrique; ainsi le problème ne peut être résolu en général avec la règle et le compas. Il nous semble qu'il n'avait pas encore été démontré rigoureusement que ces problèmes, si célèbres chez les anciens, ne fussent pas susceptibles d'une solution par les constructions géométriques auxquelles ils s'attachaient particulièrement.

La division de la circonférence en parties égales peut toujours se ramener à la résolution de l'équation $x^m - 1 = 0$, dans laquelle *m* est un nombre premier ou une puissance d'un nombre premier. Lorsque *m* est premier, l'équation $\frac{x^m - 1}{x - 1} = 0$ du degré $m - 1$ est irréductible, comme M. Gauss l'a fait voir dans ses *Disquisitiones arithmeticæ*, section VII; ainsi la division ne peut être effectuée par des constructions géométriques que si $m - 1 = 2^\alpha$. Quand *m* est de la forme a^α, on peut prouver, en modifiant légèrement la démonstration de M. Gauss que l'équation de degré $(a-1)a^{\alpha-1}$, obtenue en égalant à zéro le quotient de $x^{a^\alpha} - 1$ par $x^{a^{\alpha-1}} - 1$, est irréductible; il faudrait donc que $(a-1)a^{\alpha-1}$, fût de la forme 2^n en même temps que $a - 1$, ce qui est impossible à moins que $a = 2$. Ainsi, *la division de la circonférence en N parties ne peut être effectuée avec la règle et le compas que si les facteurs premiers de N différents de 2 sont de la forme* $2^n + 1$ *et s'ils entrent seulement à la première puissance dans ce nombre.* Ce principe est annoncé par M. Gauss à la fin de son ouvrage, mais il n'en a pas donné la démonstration.

Si l'on pose $= k + A'\sqrt[m']{a'} + A''\sqrt[m'']{a''} + etc.$, m', m'', ... étant des puissances de *2*, et *k*, A', A'', ... a', a'', ... des nombres commensurables, la valeur de *x* se construira par la ligne droite et le cercle, en sorte que *x* ne peut être racine d'une équations irréductible d'un degré *m* qui ne soit pas une puissance de *2*. Par exemple, on ne peut avoir, $x = A\sqrt[m]{a}$, si

$\left(\sqrt[m]{a}\right)^p$ est irrationnel pour $p < m$; on démontrerait facilement que *x* ne peut prendre cette valeur lors même que *m* serait une puissance de *2*. Nous retrouvons ainsi plusieurs cas particuliers des théorèmes sur les nombres incommensurables que nous avons établis ailleurs.[6]

V.

Supposons qu'un problème ait conduit à une équation de degré 2^n, $F(x) = 0$ et qu'on se soit assuré que cette équation est irréductible; il s'agit de reconnaître si la solution peut s'obtenir au moyen d'une série d'équations du second degré.

Reprenons les équations *(A)*:

$$\text{(A)} \begin{cases} x_1^2 + Ax_1 + B = 0,\ x_2^2 + A_1x_2 + B_1 = 0 \ldots, \\ x_{n-1}^2 + A_{n-2}x_{n-1} + B_{n-2} = 0,\ x_n^2 + A_{n-1}x_n + B_{n-1} = 0. \end{cases}$$

il faudra construire l'équation $f(x) = 0$, à coefficientes rationnels, qui donne toutes les valeurs de x_n et l'identifier avec l'équation donnée $F(x) = 0$. Pour faire ce calcul on remarque que A_{n-1} et B_{n-1} se ramènent à la forme $a_{n-1}x_{n-1} + a'_{n-1}$ et $b_{n-1}x_{n-1} + b'_{n-1}$, en sorte que l'élimination de x_{n-1} entre les deux dernières équations *(A)* se fait immédiatement, ce qui donne une équation de quatrième degré en x_n; on y remplacera ensuite a_{n-1} par $a''_{n-1}x_{n-2} + a'''_{n-1}$, a'_{n-1} par $a^{iv}_{n-1}x_{n-2} + a^{v}_{n-1}$, b_{n-1} par $b''_{n-1}x_{n-2} + b'''_{n-1}$, b'_{n-1} par $b^{\mathrm{iv}}_{n-1}x_{n-2} + b^{v}_{n-1}$ et A_{n-2}, B_{n-2}[7] par $a_{n-2}x_{n-2} + a'_{n-2}$, $b_{n-2}x_{n-2} + b'_{n-2}$, puis on éliminera x_{n-2} entre l'équation du 4e degré déjà obtenue et l'équation $x_{n-2}^2 + A_{n-3}x_{n-2} + B_{n-3} = 0$; et ainsi de suite. Les derniers termes des séries a_{n-1}, a'_{n-1}, a''_{n-1} ..., b_{n-1}, b'_{n-1}..., etc., doivent être des fonctions rationnelles des coefficients de $F(x) = 0$; si l'on peut leur assigner des valeurs rationnelles qui satisfassent aux équations de condition obtenues en identifiant, on reproduira les équations *(A)* dont le système équivaut à l'équation $F(x) = 0$; si les conditions ne peuvent être vérifiées en donnant des valeurs rationnelles aux indéterminées introduites, le problème ne peut être ramené au second degré.

On peut simplifier ce procédé, en supposant que les racines de chacune des équations *(A)* donnent le dernier terme de la suivante; ainsi, l'on peut prendre B_{n-1} pour l'inconnue de l'avant-dernière équation, puisque $B_{n-1} = b_{n-1}x_{n-1} + b'_{n-1}$ d'ou $x_{n-1} = \frac{B_{n-1} - b'_{n-1}}{b_{n-1}}$; de cette manière les éliminations se font plus rapidement et l'on introduit quatre quantités indéterminées dans l'équation du quatrième degré qui résulte de la première élimination, huit dans l'équation du huitième degré, etc., en sorte que les conditions obtenues en identifiant sont en même nombre que les quantités à déterminer. Mais on écarte aussi à l'avance le cas où l'une des quantités telle que b_{n-1} serait nulle, et il faut étudier ce cas séparément.

Soit, par exemple, l'équation $x^4 + px^2 + qx + r = 0$. Prenons de suite les équations du second degré sous la forme $x_1^2 + Ax_1 + B = 0$, et $x^2 + (ax_1 + a')x + x_1 = 0$; en éliminant x_1 et identifiant, on aura,

$2a' - Aa = 0, a'^2 - Aaa' - A + a^2B = p, 2aB - a'A = q, B = r,$

[6] Journal de L'École Polytechnique, Cahier XXVI.

[7] No original B_{n-1}.

d'où

$B = r, a = \frac{2q}{4r-A^2}, a' = \frac{Aq}{4r-A^2}, A^3 + pA^2 - 4rA + q^2 - 4rp = 0.$

Comme *B*, *a* et *a´*sont exprimés rationnellement au moyen de *A*, *p*, *q*, *r*, il faut et il suffit que l'équation du troisième degré en *A* ait pour racine une fonction rationnelle des données. La condition est toujours satisfaite quand $q = 0$, quels que soient *p* et *r*, car $A = -p$ satisfait alors à la dernière équation.

En prenant x_1 pour dernier terme de la deuxième équation du second degré, on a exclu de cas où ce terme serait indépendant de la racine de la première équation; mais en le traitant directement, on ne trouve aucune solution de la question qui ne soit comprise dans les équations ci-dessus.

Ainsi, par un calcul plus ou moins long, on pourra toujours s'assurer si un problème donné est susceptible d'être résolu au moyen d'une série d'équations du second degré, pourvu qu'on sache reconnaître si une équation peut être satisfaite par une fonction rationnelle des données, et si elle est irréductible. Une équation de degré *n* sera irréductible lorsqu'en cherchant les diviseurs de son premier membre de degrés *1, 2,* ... $\frac{n}{2}$, on n'en trouve aucun dont les coefficients soient fonctions rationnelles des quantités données.

La question peut donc toujours être ramenée à rechercher si une équation algébrique $F(x) = 0$ à une seule inconnue peut avoir pour racine une fonction de ce genre. Pour cela, il y a plusieurs cas à considérer. Iº Si les coefficients ne dépendent que de nombres donnés entiers ou fractionnaires, il suffira d'appliquer la méthode des racines commensurables. 2º Il peut arriver que les données représentées par les lettres *p, q, r* soient susceptibles de prendre une infinité de valeurs, sans que la condition cesse d'être remplie, comme quand elle désignent plusieurs lignes prises arbitrairement; alors, après avoir ramené l' équation *F(x) = 0* à une forme telle que ses coefficients soient des fractions entières de *p, q, r* ..., et que celui du premier terme soit l'unité, on remplacera *x* par $a_m p^m - a_{m-1} p^{m-1} + \ ... + a_0$, et l'on égalera à zéro les coefficients des différentes puissances dans le résultat; les équations obtenues en a_m,[8] a_{m-1} ... seront traitées comme l'équation en *x*, c'est-à-dire qu'on y remplacera ces quantités par des fonctions entières de q, et ainsi de suite jusqu'à ce qu'ayant épuisé toutes les lettres on soit arrivé à des équations numériques qui rentreront dans le premier cas. 3º Lorsque les données sont des nombres irrationnels, ils doivent être racines d'équations algébriques qu'on peut supposer irréductibles; dans ce cas, si l'on remplace *x* par $a_m p^m + \ ... + a_0$; dans $F(x) = 0$, le premier membre de l'équation en *p*, ainsi obtenue, devra être divisible par celui de l'équation irréductible dont le nombre *p* est racine; en exprimant que cette division se fait exactement, on arrivera à des équations en a_m, a_{m-1} ..., que l'on traitera comme l'équation $F(x) = 0$, jusqu'à ce que l'on parvienne à des équations numériques. On doit remarquer que *m* peut toujours être pris inférieur au degré de l'équation qui donne *p*.

Ces procédés sont d'une application pénible en général, mais on peut les simplifier et obtenir des résultats plus précis dans certains cas très étendus, que nous étudierons spécialement.

[8] No original a^m.

Fernando Raul Neto
Endereço: Av. da Arquitetura, s/n, CFCH – 15º andar
Cidade Universitária – Recife – PE, CEP 50.740-530
E-mail: feraneto@uol.com.br

João Paulo Barbosa
Endereço: BR 203, Km 02, s/n, Petrolina – PE, CEP: 56.328-903
E-mail: joao.barbosa@upe.br